“Panel discussion on modelling and pricing challenges”

Cyber Scenarios (columns) and affected covers (rows)

IMIA Working Group Paper 98 (16)

Cyber Pricing Cyber Scenarios with Effects to Indemnification types	Malicious Act /Targeted Virus Target: PD	Computer Malware, widespread Virus	Human Error	System Failure
	frequency estimate	frequency estimate	frequency estimate	frequency estimate
	events per year	events per year	events per year	events per year
	freq.estimate per outsourcing provider	freq.estimate per outsourcing provider	freq.estimate per outsourcing provider	freq.estimate per outsourcing provider
	events per year	events per year	events per year	events per year
	Probability	Probability	Probability	Probability
+ Privacy Breach: PII data affected				
+ Data Breach: non-PII data affected				
+ Data Insurance: Loss of own data				
+ Property Damage	100			
+ PD costs				
+ BI following PD				
+ Loss of Profit				
+ Increased cost of working				
+ Extortion due to PD threat				
+ Payment of Extortion Ransom				
+ Crisis management Fees				
+ other BI				
+ Extortion due to unknown threat				
+ other target affected through Insured's network				
+ Media Liability Issue				

- *Loss severity distribution: NLE - PML – MFL*
- *Frequency estimation*
- *Multiple coverage triggers*

costs and causes of cyber incidents – S. Romanosky, RAND, 2016

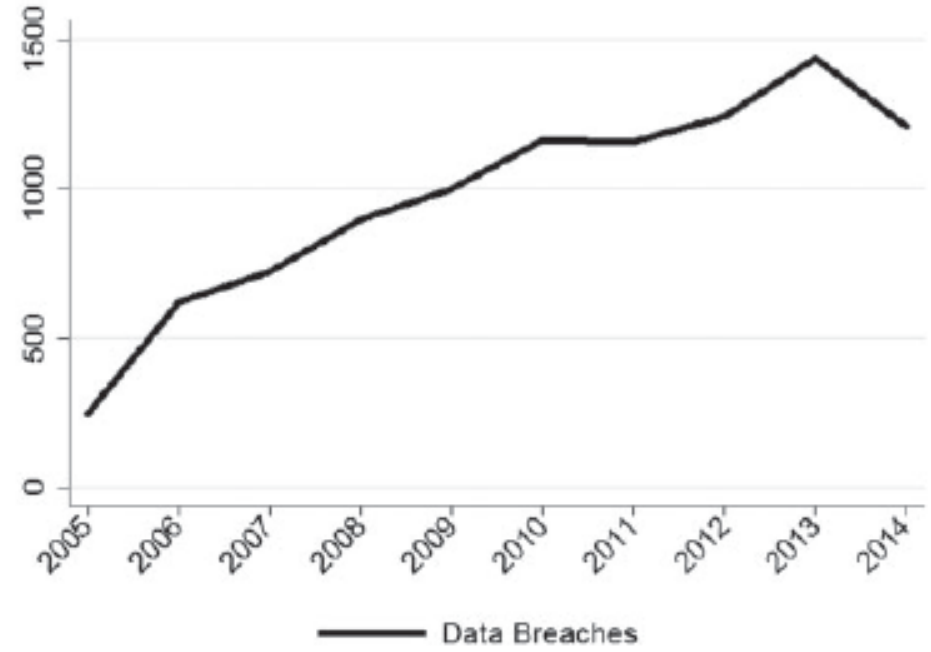
… concerns regarding … increasing rates of (cyber incidents) conflict ... with our findings that show … smaller … impact to firms that suffer (cyber) events… we find that…

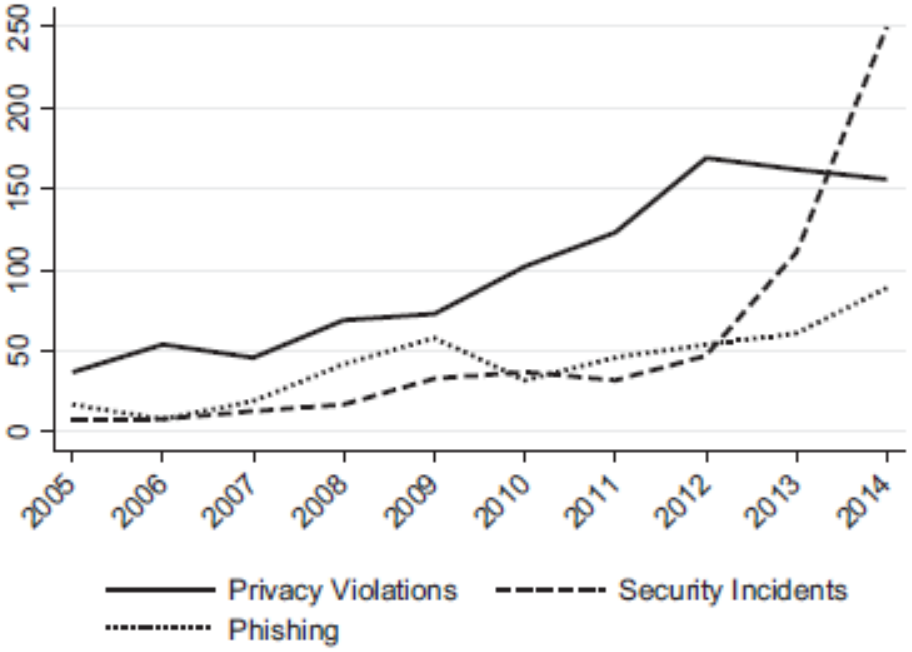
… **costs of a typical cyber incident in our sample of 12.000 cyber events (data breaches, security incidents, privacy violations, phishing crimes) is less than $200k**

- only a fraction of the millions of dollars commonly cited … this **represents only Ø 0.4% of company annual revenues**.

http://cybersecurity.oxfordjournals.org/content/cybers/early/2016/08/08/cybsec.tyw001.full.pdf

costs and causes of cyber incidents – S. Romanosky, RAND, 2016





types of cyber events.

D.B.: disclosure of PII, theft of computers, identity theft, fraud

S.I.: computers/network disruption, DoS, intellectual prop. theft, hack, extortion, BI

P.V.: collection, use, sharing of personal information

costs and causes of cyber incidents – S. Romanosky, RAND, 2016

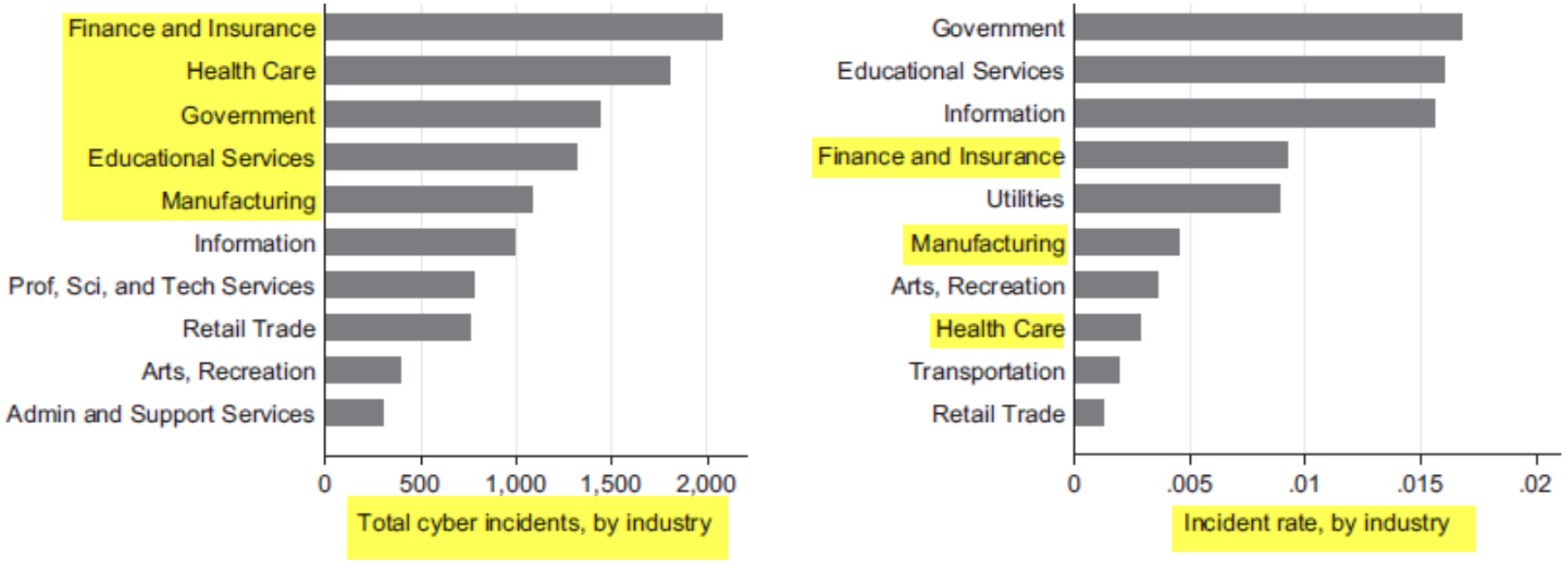


Figure 3. Cyber incidents, and rates, by industry.

costs and causes of cyber incidents – S. Romanosky, RAND, 2016

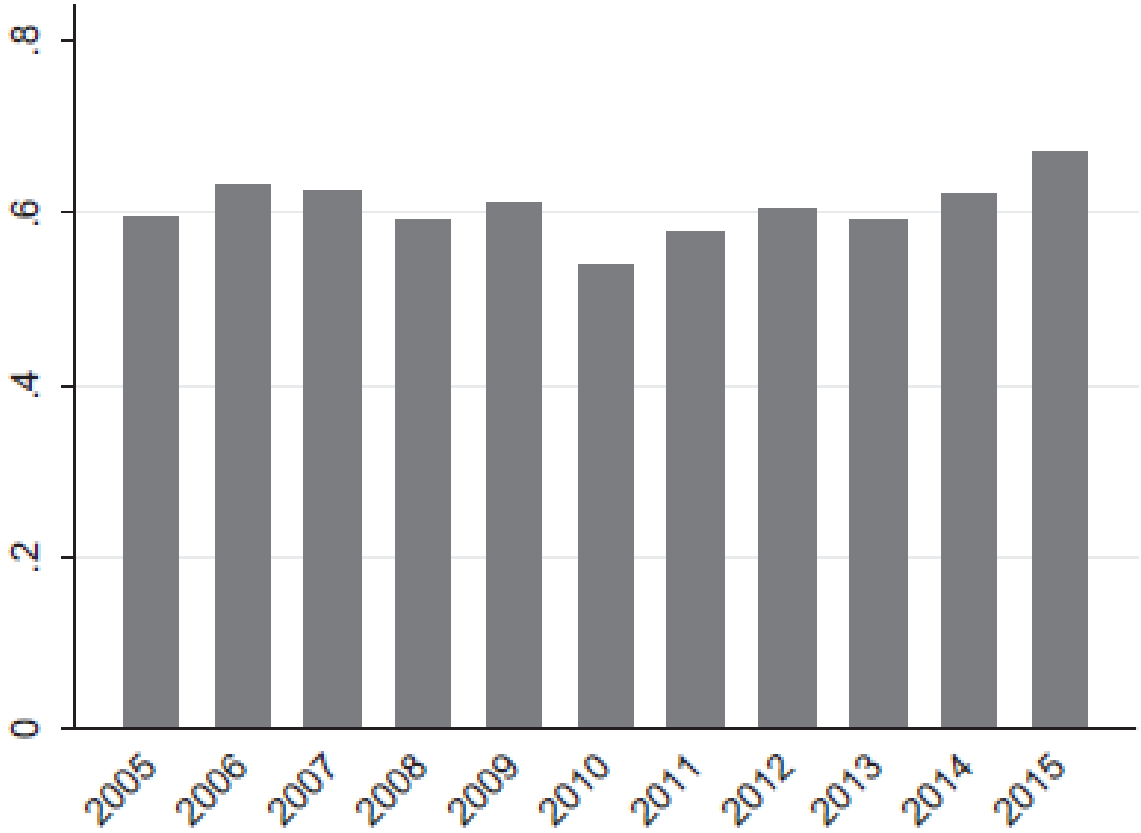


Figure 5. Rates of malicious events.

costs and causes of cyber incidents – S. Romanosky, RAND, 2016

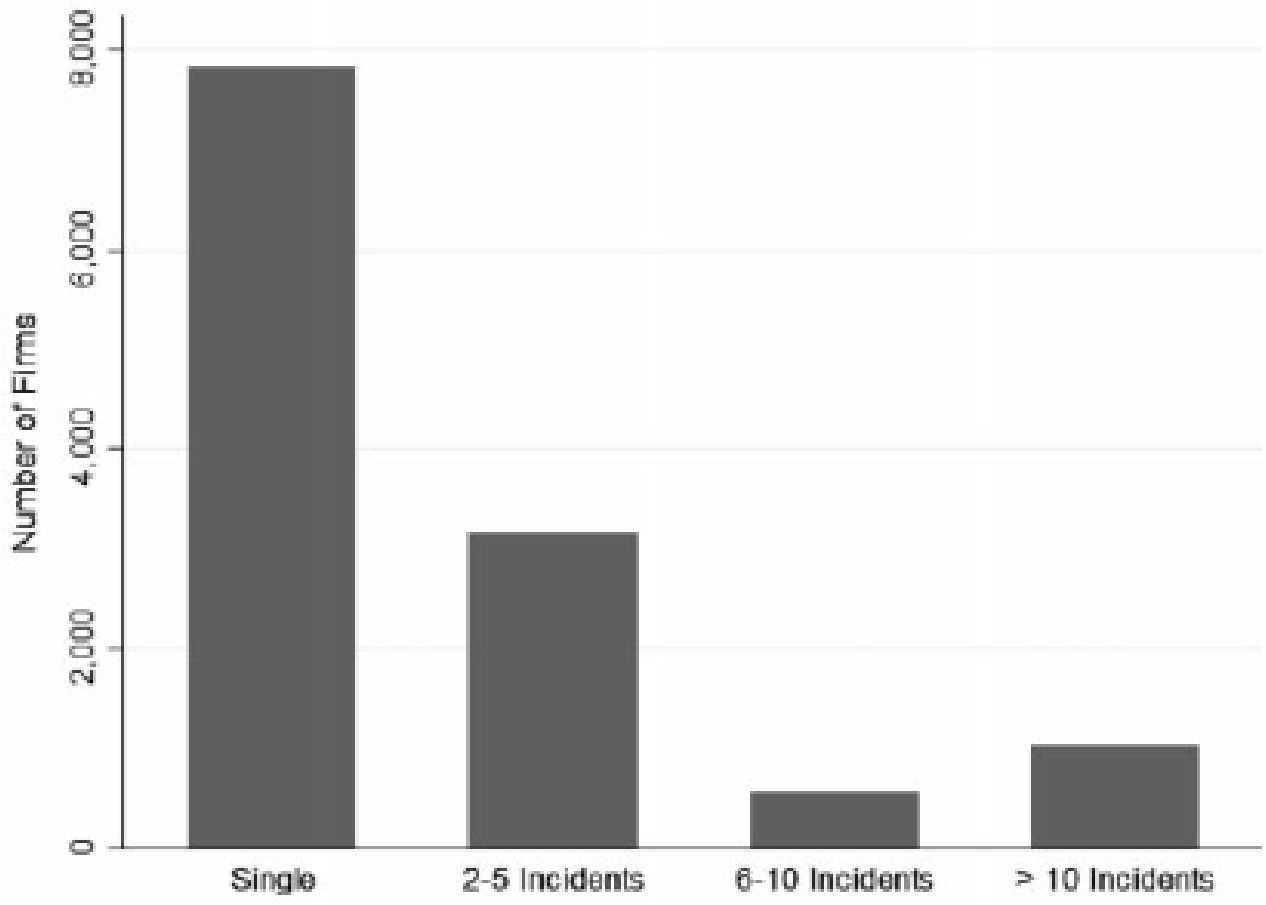
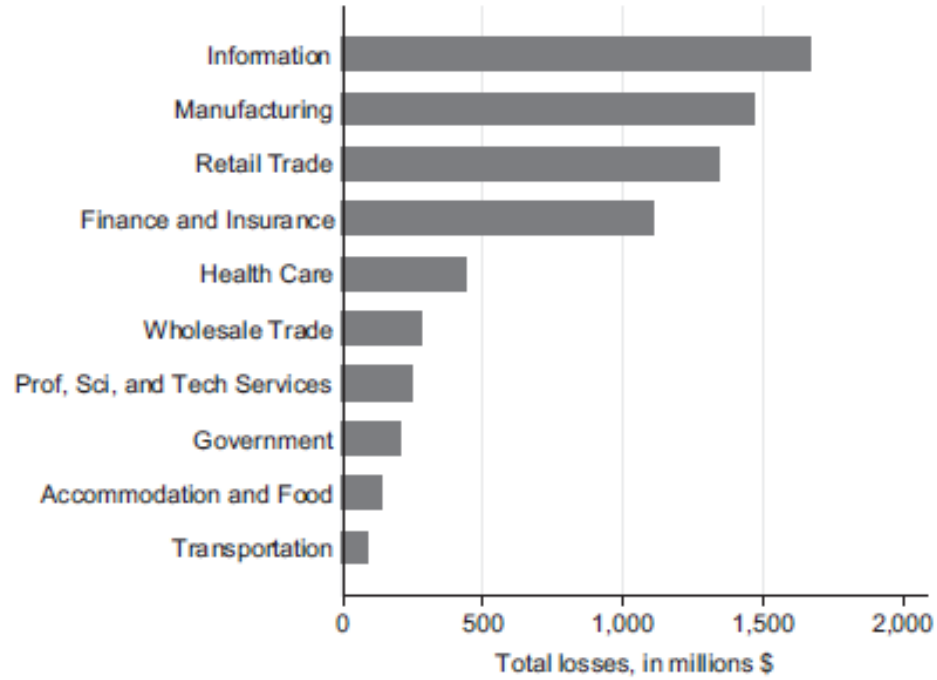


Figure 10. Distribution of repeat players.

costs and causes of cyber incidents – S. Romanosky, RAND, 2016



Losses by industry.

costs and causes of cyber incidents – S. Romanosky, RAND, 2016

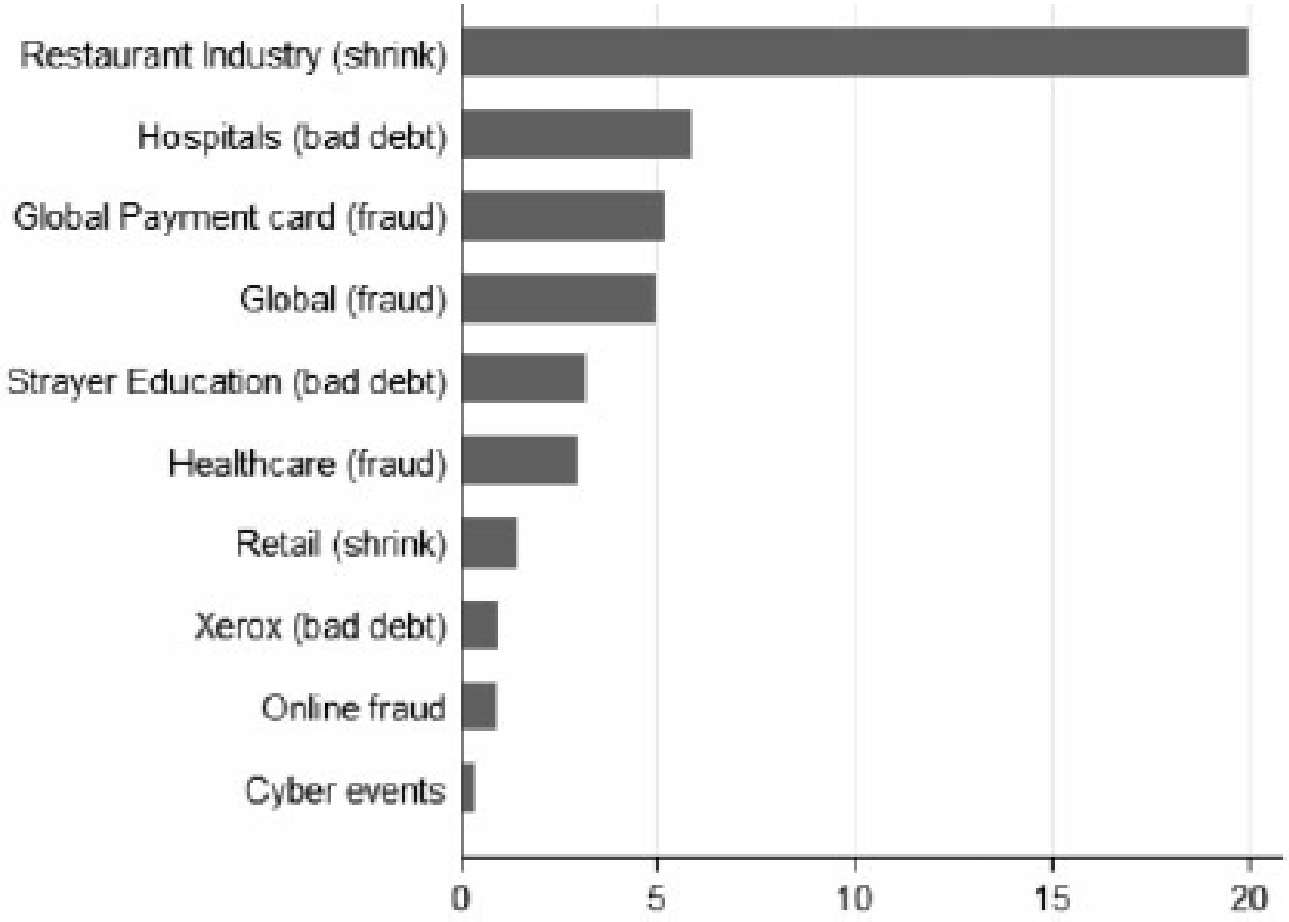


Figure 15. Loss as a percentage of revenues.

costs and causes of cyber incidents – S. Romanosky, RAND, 2016

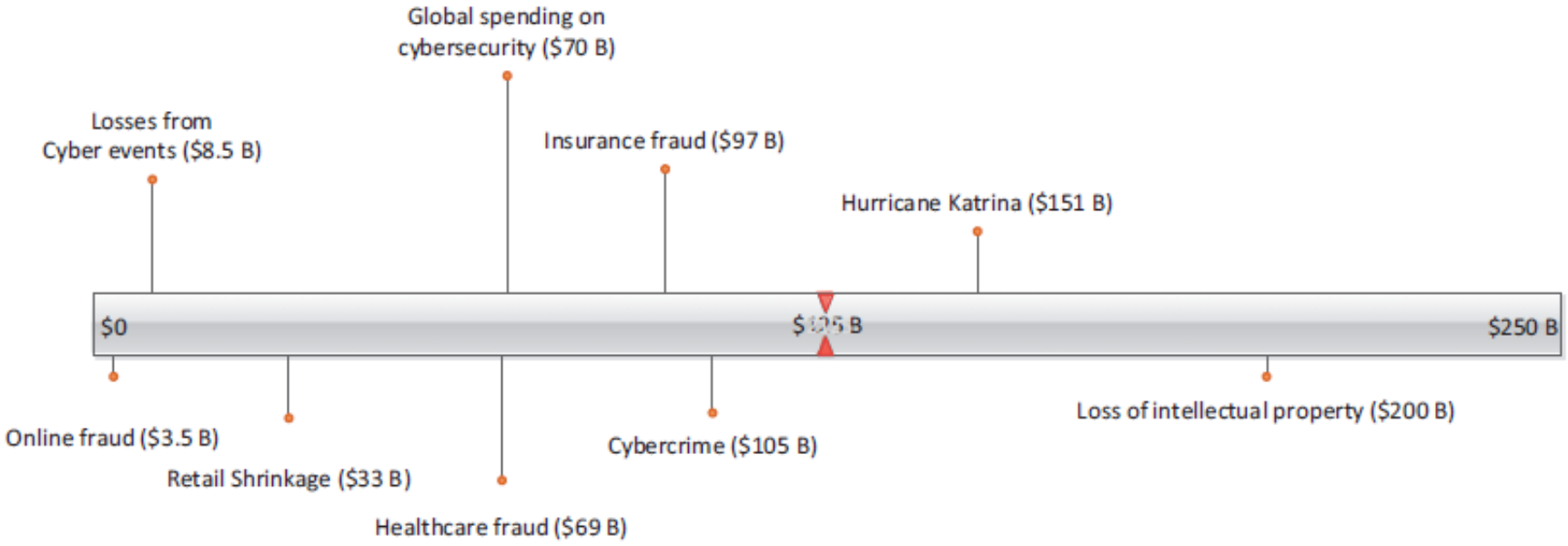


Figure 14. Relative costs and losses (annual, in billions of US dollars) (Indeed, there may be some overlap between some categories (i.e. intellectual property cyber crime). However, these descriptions are presented as informational estimates only.).

Actors and Motivations

- Cyber Risk - **man-made,** diverse and evolving
- Frequency - severity may change rapidly
- Profile of the company effects the frequency - severity
  - Revenue, size, political affiliations, location, intellectual and financial assets
  - Business decisions translate into a change in cyber exposure

- Manage “attack risk profile”
  - Monitor adversaries
  - Use threat intelligence